From:	Lemons Terry L
To:	Lipold John A; angela_camp@intuit.com; Bernie McKay; Kpickering@hrblock.com; SRyan@mwe.com; Joe.Sica@sbtpg.com; Smith Verenda; jonathan.lyon; Mathis Nancy; leann.boswell@iowa.gov; astanley4@dor.in.gov; Johnston Alec S; Ramsey Maryclaire; dransom@mwe.com; Eguren Sara L; Migazzi Donna J; Stepter Deirdre H; Collins, Thomas W (Tom); mcastro@petzent.com; Kerns Chris D; Eldridge Michelle L; Pryde Joan A; Allen Sarah; Ashley_McMahon@intuit.com; Asper Damon C; Nadal Yadira G; Pachner Anny K; Cresson Frederick L; Fulmer, Michael (TAX); "larry@agccpa.com"; Cynthia Zaki; Burkhart Brent L; Brennan Lynn M; James.Carson@po.state.ct.us; Gazzale, James (TAX); jams@nsacct.org; "johncharlescraig@gmail.com" (johncharlescraig@gmail.com); Mercado Wayne R; Fallon, Laura A (TAX); Koslowsky, Erica L (TAX); Hardy Mel; Bond, Shannon; Tim Hugo@capnet.org (Tim.Hugo@capnet.org); Hull, Vickie (Vickie.Hull@timhugo.com); Michael Blache; Maser Peter E; Netram, Melissa; Ferguson Shane; Eubanks, Daniel; Romaniello Margaret A; Fletcher, Julia A; De Ford, Azalea; Burch Stephanie C; Russell, Christopher (DOR); Landis, Emily; Reynolds Jodie M; Andrews Sheila L; Cain, Michelle L; Mark Castro; Connelly Karen A; Courtney Decker; lynne.riley@dor.ga.gov; Sharonne Bonardi; Mealy Filomena; Waldron, Susan; Crews Craig E; btaylor@azdor.gov; Sincox Terri; brownlua@gvsu.edu; Joe Sica; Eric Inkrott; Leas Matthew F; Connelly Karen A
Subject:	Tax Security 101 Campaign - Installments 7 and 8
Date:	Friday, August 17, 2018 12:51:00 PM
Attachments:	image001.jpg image002.jpg IR 2018-#7 TaxSecurity101EducateEmployees.doc IR 2018-#8 TaxSecurity101legalobligations1.doc

---

Summit Communications Team – Attached are the next two installments in the Tax Security 101 campaign for weeks seven and eight, focused on educating employees and a reminder on data security plan requirements. We're sharing these as fyi at this point; final versions will be issued over the next two weeks (No. 7 will be Tuesday, No. 8 the following Tuesday).

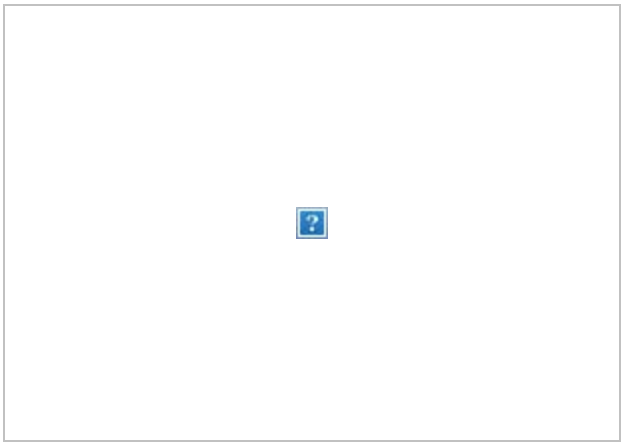
A couple of additional notes:
*Summit members are welcome to use the finals either "as is" or with their own branding through their channels.
*We will have Spanish language versions of these available on the day of release.
*All of the English versions of the 101 series can be found on this page on IRS.gov: https://www.irs.gov/newsroom/protect-your-clients-protect-yourself-tax-security-101 . The Spanish language versions are at: https://www.irs.gov/es/newsroom/protect-your-clients-protect-yourself-tax-security-101
*For those on Twitter, we are using #TaxSecurity101 and #SecuritySummit as hashtags.
*Also using some of these images on Twitter to promote the campaign.

Thanks, and have a great weekend.
Terry

Tax Security 101

New Security Summit campaign helps protect taxpayer data.

Link: https://www.irs.gov/newsroom/protect-your-clients-protect-yourself-tax-security-101



Tax Security 101

Tax professionals: Protect Your Clients; Protect Yourself.

Link: https://www.irs.gov/newsroom/protect-your-clients-protect-yourself-tax-security-101

INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.317.4000
www.irs.gov/newsroom | Public Contact: 800.829.1040

Tax Security 101: Security Summit Urges Tax Pros to Educate All Employees about Data Security and Computing Safeguards

IR-2018-XX, Aug. XX, 2018

WASHINGTON – The IRS and its Security Summit partners today called on tax professionals to step up security education for all office employees, including themselves, to better protect taxpayer data and help prevent fraudulent return filings.

The warning from the IRS, state tax agencies and the nation's tax industry follows an increase this year in reports of data thefts from tax professionals. The Security Summit partners remind professionals that their clients' data and their businesses are only as secure as their least informed employee.

This is the seventh in a series called Protect Your Clients; Protect Yourself: Tax Security 101. The Security Summit awareness campaign is intended to provide tax professionals with the basic information they need to better protect taxpayer data and to help prevent the filing of fraudulent tax returns.

Although the Security Summit is making progress against tax-related identity theft, cybercriminals continue to evolve, and data thefts at tax professionals' offices is on the rise. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder to detect.

The IRS continues to see an increase in the number of data thefts reported by tax professionals. Through Aug. 9, there had been 217 tax professionals reporting data thefts this year, a 30 percent increase from 167 through the same period in 2017.

All employees should be aware of the dangers related to phishing emails, especially spear phishing emails. An employee does not have to be a tax preparer to accidentally disclose critical password information or download malware that could infect and impact all office computers and risk the theft of client data.

All professional tax return preparers must adhere to the "Safeguards Rule" set out by the Gramm-Leach-Bliley Act of 1999 and administered by the Federal Trade Commission. The FTC sets out a series of suggested areas to address, including for employee management and training. The FTC suggests following this list and the IRS has added some updates specifically for tax professionals:

- Check references or doing background checks before hiring employees who will have access to customer information.
- Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.

- Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
- Control access to sensitive information by requiring employees to use “strong” passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) *(IRS suggestion: passwords should be a minimum of eight characters.)*
- Use password-activated screen savers to lock employee computers after a period of inactivity.
- Develop policies for appropriate use and protection of laptops, personal digital assistants, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.
- Train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, including:
    - Locking rooms and file cabinets where records are kept;
    - Not sharing or openly posting employee passwords in work areas;
    - Encrypting sensitive customer information when it is transmitted electronically via public networks;
    - Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
    - Reporting suspicious attempts to obtain customer information to designated personnel.
- Regularly remind all employees of your company’s policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.
- Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
- Impose disciplinary measures for security policy violations.
- Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

All employees within a tax professional's office should familiarize themselves with FTC regulations and IRS publications and websites that will help increasing security awareness.

To improve data security awareness by all tax professionals, the IRS will host an upcoming webinar this fall. The focus will be on the same topics as this series: "Protect Your Clients; Protect Yourself: Tax Security 101." Although tax preparers will be eligible for one CPE credit, the IRS welcomes tax professionals and their employees. Protecting taxpayer information takes all of us working together.

The Security Summit reminds all professional tax preparers that you must have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule. You also can get help with security recommendations by reviewing the recently revised IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security: the Fundamentals by the National Institute of Standards and Technology.

Publication 5293, Data Security Resource Guide for Tax Professionals, provides a compilation of data theft information available on IRS.gov. Also, tax pros should stay connected to the IRS through subscriptions to e-News for Tax Professionals, QuickAlerts and Social Media.

INTERNAL REVENUE SERVICE
IRS News Release

Media Relations Office | Washington, D.C. | Media Contact: 202.317.4000
www.irs.gov/newsroom | Public Contact: 800.829.1040

Tax Security 101: Security Summit Reminds Professional Tax Preparers of Data Security Plan Requirements

IR-2018-XX, Jan. XX, 2018

WASHINGTON – The Internal Revenue Service and Security Summit partners reminded tax professionals that protecting taxpayer information isn't just good for the clients and good for business – it's also the law.

The Summit partners urged tax professionals to be aware of their obligations to protect client data and to cooperate with any IRS investigation related to data theft.

The IRS has a number of publications to help tax pros navigate tax-related rules and regulations related to protecting data. In addition, the IRS, state tax agencies and the tax industry today reminded tax return preparers that a 1999 law requires that they create and implement a data security plan.

The Summit partners urged tax professionals to be aware of their obligations to protect client data and to cooperate with any IRS investigation related to data theft.

This isthe eighth in a series called "Protect Your Clients; Protect Yourself: Tax Security 101." The Security Summit awareness campaign is intended to provide tax professionals with the basic information they need to better protect taxpayer data and to help prevent the filing of fraudulent tax returns.

Although the Security Summit is making progress against tax-related identity theft, cybercriminals continue to evolve, and data thefts at tax professionals' offices is on the rise. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder to detect.

The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley (GLB) Act, gives the Federal Trade Commission authority to set information safeguard regulations for various entities, including professional tax return preparers.

According to the FTC Safeguards Rule, tax return preparers must create and enact security plans to protect client data. Failure to do so may result in an FTC investigation. The IRS also may treat a violation of the FTC Safeguards Rule as a violation of IRS Revenue Procedure 2007-40, which sets the rules for tax professionals participating as an Authorized IRS e-File Provider.

In addition, members of the the IRS Electronic Tax Administration Advisory Committee (ETAAC) in June noted that they believe "far fewer than half of tax professionals are aware of their

responsibilities under the FTC Safeguards rule and that even fewer professionals …have implemented required security practices."

The FTC-required information security plan must be appropriate to the company's size and complexity, the nature and scope of its activities and the sensitivity of the customer information it handles. According to the FTC, each company, as part of its plan, must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The FTC says the requirements are designed to be flexible so that companies can implement safeguards appropriate to their own circumstances. The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operations.

The IRS has revised Publication 4557 to detail critical security measures that all tax professionals should enact. The publication also includes information on how to comply with the FTC Safeguards Rule, including a checklist of items for a prospective data security plan.

The IRS and certain Internal Revenue Code (IRC) sections also focus on protection of taxpayer information and requirements of tax professionals. Here are a few examples:

IRS Publication 3112 - IRS e-File Application and Participation, states: Safeguarding of IRS e-file from fraud and abuse is the shared responsibility of the IRS and Authorized IRS e-file Providers. Providers must be diligent in recognizing fraud and abuse, reporting it to the IRS, and preventing it when possible. Providers must also cooperate with the IRS' investigations by making available to the IRS upon request, information and documents related to returns with potential fraud or abuse.

IRC, Section 7216 - This provision imposes criminal penalties on any person engaged in the business of preparing or providing services in connection with the preparation of tax returns who knowingly or recklessly makes unauthorized disclosures or uses of information furnished tothem in connection with the preparation of an income tax return.

IRC, Section 6713 - This provision imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.

Rev. Proc. 2007-40 - This procedure requires Authorized IRS e-file Providers to have security systems in place to prevent unauthorized access to taxpayer accounts and personal information by third parties. It also specifies that violations of the GLB Act and the implementing rules and regulations promulgated by the FTC, as well as violations of the non-disclosure rules contained in IRC sections 6713 and 7216 or the regulations promulgated thereunder are considered violations

of Revenue Procedure 2007-40, and are subject to penalties or sanctions specified in the Revenue Procedure.

Many state laws govern or relate to the privacy and security of financial data, which includes taxpayer data. They extend rights and remedies to consumers by requiring individuals and businesses that offer financial services to safeguard nonpublic personal information. For more information on state laws that your business must follow, consult state laws and regulations.

In some states, data thefts must be reported to various authorities. To help tax professionals find where to report data security incidents at the state level, the Federation of Tax Administrators has created a special page at https://taxadmin.memberclicks.net/state-id-theft-resources with state-by - state listings. To notify the IRS in case of data theft, contact your local Stakeholder Liaison.

Tax professionals also can get help with security recommendations by reviewing the recently revised IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security: the Fundamentals by the National Institute of Standards and Technology.

Publication 5293, Data Security Resource Guide for Tax Professionals, provides a compilation data theft information available on IRS.gov. Also, tax pros should stay connected to the IRS through subscriptions to e-News for Tax Professionals, QuickAlerts and Social Media.

To improve data security awareness by all tax professionals, the IRS will host an upcoming webinar this fall. The focus will be on the same topics as this series: “Protect Your Clients; Protect Yourself: Tax Security 101.” Although tax preparers will be eligible for one CPE credit, the IRS others working on tax issues to attend. Protecting taxpayer information takes all of us working together.